



Check Point

156-215.77 Exam

Check Point Certified Security Administrator Exam

Thank you for Downloading 156-215.77 exam PDF Demo

You can Buy Latest 156-215.77 Full Version Download

<https://www.certkillers.net/Exam/156-215.77>

<https://www.certkillers.net>

Version: 14.0

Question: 1

You manage a global network extending from your base in Chicago to Tokyo, Calcutta and Dallas. Management wants a report detailing the current software level of each Enterprise class Security Gateway. You plan to take the opportunity to create a proposal outline, listing the most cost-effective way to upgrade your Gateways.

Which two SmartConsole applications will you use to create this report and outline?

- A. SmartView Tracker and SmartView Monitor
- B. SmartLSM and SmartUpdate
- C. SmartDashboard and SmartView Tracker
- D. SmartView Monitor and SmartUpdate

Answer: D

Question: 2

Your bank's distributed R77 installation has Security Gateways up for renewal.

Which SmartConsole application will tell you which Security Gateways have licenses that will expire within the next 30 days?

- A. SmartView Tracker
- B. SmartPortal
- C. SmartUpdate
- D. SmartDashboard

Answer: C

Question: 3

When launching SmartDashboard, what information is required to log into R77?

- A. User Name, Management Server IP, certificate fingerprint file
- B. User Name, Password, Management Server IP
- C. Password, Management Server IP
- D. Password, Management Server IP, LDAP Server IP

Answer: B

Question: 4

Message digests use which of the following?

- A. DES and RC4
- B. IDEA and RC4
- C. SSL and MD4
- D. SHA-1 and MD5

Answer: D

Question: 5

Which of the following is a hash algorithm?

- A. 3DES
- B. IDEA
- C. DES
- D. MD5

Answer: D

Question: 6

Which of the following uses the same key to decrypt as it does to encrypt?

- A. Asymmetric encryption
- B. Dynamic encryption
- C. Certificate-based encryption
- D. Symmetric encryption

Answer: D

Question: 7

You believe Phase 2 negotiations are failing while you are attempting to configure a site-to-site VPN with one of your firm's business partners.

Which SmartConsole application should you use to confirm your suspicions?

- A. SmartDashboard
- B. SmartUpdate
- C. SmartView Status
- D. SmartView Tracker

Answer: D

Question: 8

A digital signature:

- A. Guarantees the authenticity and integrity of a message.
- B. Automatically exchanges shared keys.
- C. Decrypts data to its original form.
- D. Provides a secure key exchange mechanism over the Internet.

Answer: A

Question: 9

Which component functions as the Internal Certificate Authority for R77?

- A. Security Gateway
- B. Management Server
- C. Policy Server
- D. SmartLSM

Answer: B

Question: 10

The customer has a small Check Point installation which includes one Windows 2008 server as the SmartConsole and a second server running GAIA as both Security Management Server and the Security Gateway. This is an example of a(n):

- A. Distributed Installation
- B. Unsupported configuration
- C. Hybrid Installation
- D. Stand-Alone Installation

Answer: D

Question: 11

The customer has a small Check Point installation which includes one Windows 7 workstation as the SmartConsole, one GAIA device working as Security Management Server, and a third server running SecurePlatform as Security Gateway. This is an example of a(n):

- A. Hybrid Installation
- B. Unsupported configuration
- C. Stand-Alone Installation
- D. Distributed Installation

Answer: D

Question: 12

The customer has a small Check Point installation which includes one Windows 2008 server as SmartConsole and Security Management Server with a second server running GAIA as Security Gateway. This is an example of a(n):

- A. Stand-Alone Installation.
- B. Distributed Installation.
- C. Unsupported configuration.
- D. Hybrid Installation.

Answer: B

Question: 13

When doing a Stand-Alone Installation, you would install the Security Management Server with which other Check Point architecture component?

- A. None, Security Management Server would be installed by itself.
- B. SmartConsole
- C. SecureClient
- D. Security Gateway

Answer: D

Question: 14

Tom has been tasked to install Check Point R77 in a distributed deployment. Before Tom installs the systems this way, how many machines will he need if he does NOT include a SmartConsole machine in his calculations?

- A. Three machines
- B. One machine
- C. Two machines
- D. One machine, but it needs to be installed using SecurePlatform for compatibility purposes

Answer: C

Question: 15

Which command allows Security Policy name and install date verification on a Security Gateway?

- A. fw show policy
- B. fw stat -l
- C. fw ctl pstat -policy
- D. fw ver -p

Answer: B

Question: 16

You have two rules, ten users, and two user groups in a Security Policy. You create database version 1 for this configuration. You then delete two existing users and add a new user group. You modify one rule and add two new rules to the Rule Base. You save the Security Policy and create database version 2. After awhile, you decide to roll back to version 1 to use the Rule Base, but you want to keep your user database.

How can you do this?

- A. Run fwm dbexport -l filename. Restore the database. Then, run fwm dbimport -l filename to import the users.
- B. Run fwm_dbexport to export the user database. Select restore the entire database in the Database Revision screen. Then, run fwm_dbimport.
- C. Restore the entire database, except the user database, and then create the new user and user group.
- D. Restore the entire database, except the user database.

Answer: D

Question: 17

Which feature or command provides the easiest path for Security Administrators to revert to earlier versions of the same Security Policy and objects configuration?

- A. Database Revision Control
- B. Policy Package management
- C. dbexport/dbimport
- D. upgrade_export/upgrade_import

Answer: A

Question: 18

Your Security Management Server fails and does not reboot. One of your remote Security Gateways managed by the Security Management Server reboots.

What occurs with the remote Gateway after reboot?

- A. Since the Security Management Server is not available, the remote Gateway cannot fetch the Security Policy. Therefore, all traffic is allowed through the Gateway.
- B. Since the Security Management Server is not available, the remote Gateway cannot fetch the Security Policy. Therefore, no traffic is allowed through the Gateway.
- C. The remote Gateway fetches the last installed Security Policy locally and passes traffic normally. The Gateway will log locally, since the Security Management Server is not available.
- D. Since the Security Management Server is not available, the remote Gateway uses the local

Security Policy, but does not log traffic.

Answer: C

Question: 19

How can you configure an application to automatically launch on the Security Management Server when traffic is dropped or accepted by a rule in the Security Policy?

- A. SNMP trap alert script
- B. Custom scripts cannot be executed through alert scripts.
- C. User-defined alert script
- D. Pop-up alert script

Answer: C

Question: 20

Which of the following is NOT useful to verify whether or not a Security Policy is active on a Gateway?

- A. fw ctl get string active_secpol
- B. fw stat
- C. cpstat fw -f policy
- D. Check the Security Policy name of the appropriate Gateway in SmartView Monitor.

Answer: A

Question: 21

Exhibit:

1. Simplified mode Rule Bases
2. Traditional mode Rule Bases
3. SecurePlatform WebUI Users
4. SIC certificates
5. SmartView Tracker audit logs
6. SmartView Tracker traffic logs
7. Implied Rules
8. IPS Profiles
9. Blocked connections
10. Manual NAT rules
11. VPN communities
12. Gateway route table
13. Gateway licenses

Of the following, what parameters will not be preserved when using Database Revision Control?

- A. 2, 4, 7, 10, 11
- B. 3, 4, 5, 6, 9, 12, 13
- C. 5, 6, 9, 12, 13
- D. 1, 2, 8, 10, 11

Answer: B

Question: 22

You are about to test some rule and object changes suggested in an R77 news group.
Which backup solution should you use to ensure the easiest restoration of your Security Policy to its previous configuration after testing the changes?

- A. Manual copies of the directory \$FWDIR/conf
- B. upgrade_export command
- C. Database Revision Control
- D. GAiA backup utilities

Answer: C

Question: 23

You plan to create a backup of the rules, objects, policies, and global properties from an R77 Security Management Server. Which of the following backup and restore solutions can you use?

1. `upgrade_export` and `upgrade_import` utilities
 2. Database revision control
 3. SecurePlatform backup utilities
 4. Policy package management
 5. Manual copies of the `$CPDIR/conf` directory
- A. 2, 4, and 5
B. 1, 2, 3, 4, and 5
C. 1, 2, and 3
D. 1, 3, and 4

Answer: C

Question: 24

Which R77 feature or command allows Security Administrators to revert to earlier Security Policy versions without changing object configurations?

- A. `upgrade_export/upgrade_import`
- B. `fwm dbexport/fwm dbimport`
- C. Database Revision Control
- D. Policy Package management

Answer: C

Question: 25

What must a Security Administrator do to comply with a management requirement to log all traffic accepted through the perimeter Security Gateway?

- A. In Global Properties > Reporting Tools check the box Enable tracking all rules (including rules marked as None in the Track column). Send these logs to a secondary log server for a complete logging history. Use your normal log server for standard logging for troubleshooting.
- B. Install the View Implicit Rules package using SmartUpdate.
- C. Define two log servers on the R77 Gateway object. Enable Log Implied Rules on the first log server. Enable Log Rule Base on the second log server. Use SmartReporter to merge the two log server records into the same database for HIPPA log audits.

D. Check the Log Implied Rules Globally box on the R77 Gateway object.

Answer: A

Question: 26

Which utility allows you to configure the DHCP service on GAIa from the command line?

- A. ifconfig
- B. sysconfig
- C. cpconfig
- D. dhcp_cfg

Answer: B

Question: 27

The third-shift Administrator was updating Security Management Server access settings in Global Properties and testing. He managed to lock himself out of his account.

How can you unlock this account?

- A. Type fwm unlock_admin from the Security Management Server command line.
- B. Type fwm unlock_admin -u from the Security Gateway command line.
- C. Type fwm lock_admin -u <account name> from the Security Management Server command line.
- D. Delete the file admin.lock in the Security Management Server directory \$FWDIR/tmp/.

Answer: C

Question: 28

The third-shift Administrator was updating Security Management Server access settings in Global Properties. He managed to lock all administrators out of their accounts.

How should you unlock these accounts?

- A. Delete the file admin.lock in the Security Management Server directory \$FWDIR/tmp/.
- B. Reinstall the Security Management Server and restore using upgrade_import.
- C. Type fwm lock_admin -ua from the Security Management Server command line.
- D. Login to SmartDashboard as the special cpconfig_admin user account; right-click on each administrator object and select unlock.

Answer: C

Question: 29

You are the Security Administrator for ABC-Corp. A Check Point Firewall is installed and in use on GAI

- A. You are concerned that the system might not be retaining your entries for the interfaces and

routing configuration. You would like to verify your entries in the corresponding file(s) on GAIA. Where can you view them? Give the BEST answer.

- A. /etc/sysconfig/netconf.C
- B. /etc/conf/route.C
- C. /etc/sysconfig/network-scripts/ifcfg-ethx
- D. /etc/sysconfig/network

Answer: A

Question: 30

When using GAIA, it might be necessary to temporarily change the MAC address of the interface eth0 to 00:0C:29:12:34:56. After restarting the network the old MAC address should be active. How do you configure this change?

```
# IP link set eth0 down
# IP link set eth0 addr 00:0C:29:12:34:56
# IP link set eth0 up
```

As expert user, issue these commands:

```
(conf
:conns
: (conn
:hwaddr ("00:0C:29:12:34:56"))
```

- A. Edit the file /etc/sysconfig/netconf.C and put the new MAC address in the field
- B. As expert user, issue the command:
- C. # IP link set eth0 addr 00:0C:29:12:34:56
- D. Open the WebUI, select Network > Connections > eth0. Place the new MAC address in the field Physical Address, and press Apply to save the settings.

Answer: C

Thank You for trying 156-215.77 PDF Demo

To Buy Latest 156-215.77 Full Version Download visit link below

<https://www.certkillers.net/Exam/156-215.77>

Start Your 156-215.77 Preparation

[Limited Time Offer] Use Coupon “CKNET” for Further discount on your purchase. Test your 156-215.77 preparation with actual exam questions.

<https://www.certkillers.net>